Enabling HTTPG in GT 4.2.x Java WS Core

This patch is being provided to ESG for enabling use of HTTPG protocol in GT 4.2.x code.

- The patch is generated against globus_4_2_branch code on date specified in patch file name
- It does not fix all inherent services to use httpg, but only change the container code to use httpg on port 8443.
- The sample Secure Counter Service has been modified to use the httpg protocol.

1. Applying the patch from CVS source:

- Checkout source code from repository: cvs co -r globus_4_2_branch wsrf/java wsrf/build.xml wsrf/schema authorization
- cd wsrf
- Download patch : wget http://www.mcs.anl.gov/~ranantha/esg/bestMan/enableHttpg-20081007.tar.gz
- tar xvfz enableHttpg-200810-7.tar.gz
- patch -p0 -i enableHttpg-20081007.patch
- export GLOBUS_LOCATION /location/to/install
- ant cleanAll all

2. Applying the patch on GT 4.2.1 release:

- Download Java WS Core Source installer. The downloaded file will be named ws-core-4.2.1-src.tar.gz
- Untar and the directory will be ws-core-4.2.1 and authorization-4.2.1
- cd ws-core-4.2.1
- Download patch : wget http://www.mcs.anl.gov/~ranantha/esg/bestMan/enableHttpg-20081007.tar.gz
- tar xvfz enableHttpg-200810-7.tar.gz
- patch -p0 -i enableHttpg-20081007.patch
- export GLOBUS_LOCATION /location/to/install
- ant cleanAll all

3. Container details:

- Using shipped container start up clients, the container will use httpg on port 8443
- Valid credential, either configured using container security descriptor or default proxy must be present.

4. Service details:

- Service endpoint will container https protocol
- To access delegated credential in the service, use the following:

  ```
  import org.globus.wsrf.security.SecurityManager;
  ...
  SecurityManager manager = SecurityManager.getManager();
  Subject subject = manager.getPeerSubject();
  ```
- Note that the above requires presence of a valid MessageContext object, which is available whenever a call is received on the service, that is with in your service operation code.

- To setup the caller's delegated credentials to be used for all remote calls from an operation, use the run-as configuration as described in Run-as configuration The description for GSI Secure Conversation in Table 3 describes the functionality that will seen with use of HTTPG protocol.
- The text for GSI Secure Conversation under section Delegation is also applicable to HTTPG.

5. Client details:

- To configure use of httpg in clients, a call to org.globus.wsrf.utils.Util.registerTransport(); is required once per JVM.
- For authorization, text described for GSI Secure Conversation and Secure Transport in Configuring Client Authorization should be used. For example:
  import org.globus.axis.gsi.GSIConstants;
  import org.globus.gsi.gssapi.auth.SelfAuthorization;
  ...
  ((Stub)port)._setProperty(GSIConstants.GSI_AUTHORIZATION, SelfAuthorization.getInstance());
- The following are authorization scheme implementations shipped with the toolkit: GSI Client Authorization Schemes. Note that NoAuthorization cannot be used with delegation. Custom schemes can be used by implementing the interface org.globus.gsi.gssapi.auth.Authorization.
- Client can choose to delegate its credential by setting up property on the stub. Property 4 in "Table 1. Client side security properties" in document Client delegation property, describes how this can be setup.

6. Support:

This protocol and patch and is not supported by Globus Toolkit.

Document Date: October 7 2008